Title	PRIMES is in P : after M. Agrawal, N. Kayal, N. Saxena (Algebraic Aspects of Coding Theory and Cryptography)
Author(s)	酒井, 隆行
Citation	数理解析研究所講究録 (2004), 1361: 51-55
Issue Date	2004-04
URL	http://hdl.handle.net/2433/25258
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1361 巻 2004 年 51-55

PRIMES is in P

(after M.Agrawal, N.Kayal, N.Saxena)

東京大学大学院数理科学研究科　酒井 隆行 (Takayuki Sakai)
Graduate School of Mathematical Sciences,
University of Tokyo

1　はじめに

2002 年 8 月、Agarwal, Kayal, Saxena の三氏により、素数判定を多項式時間で行うアルゴリズムが示された [1]。それまでにも、Miller-Rabin 法のように確率的に素数判定を行うアルゴリズムなどは知られていたが、確定的多項式時間で実行されるアルゴリズムは AKS 法が初めてである。この素数判定法がどのようなアイデアに基づいているかを紹介する。

2　Fermat の小定理から AKS 法へ

まずは Fermat の小定理をそのまま素数判定に利用することを考える。

Theorem 2.1 (*Fermat* の小定理)
$a, n \in \mathbf{N}, (a,n) = 1$ とする。このとき、

$$n \text{ が素数} \Rightarrow a^{n-1} \equiv 1 \pmod{n}$$

である。

Fermat の小定理の逆が成り立つ、すなわち、$a^{n-1} \equiv 1 \pmod{n}$ が成り立つとき、n が素数となるならば、これで素数判定が行える。ところが、実際には $a^{n-1} \equiv 1 \pmod{n}$ を満たす自然数 a と合成数 n が存在する。このような n は底が a の擬素数と呼ばれる。

次に、複数の a について $a^{n-1} \equiv 1 \pmod{n}$ が成り立つかを検証することにより、n が合成数である可能性を排除できないかと考える。ところが、n と互いに素な全ての a について、底が a の擬素数となるような合成数 n (Carmichael 数と呼ばれる) が存在するため、この方法でも素数判定を行うことは出来ない。

そこで、Fermat の小定理の次のような一般化を利用する。

Lemma 2.2
$a \in \mathbf{Z}, n \in \mathbf{N}, n \geq 2, (a,n) = 1$ とする。このとき、

$$n \text{ が素数} \Leftrightarrow (X+a)^n \equiv X^n + a \pmod{n} \quad \cdots (※)$$

である。

proof.
$\Rightarrow$ は明らか。$\Leftarrow$ を示す。
n を合成数と仮定する。n の素因数 $q(\neq 1,n)$ について $q^k||n$ であるとする。
X^q の係数は $\binom{n}{q}a^{n-q}$ となるが、$q^k \nmid \binom{n}{q}$ かつ $(a,q)=1$ より、$q^k \nmid \binom{n}{q}a^{n-q}$ である。
従って、n が合成数のとき、$(X+a)^n \not\equiv X^n+a \pmod{n}$ となる。■

Lemma2.2 により、(※) の合同式が成り立つかどうかを調べれば素数判定が行えることが分かったが、(※) の左辺は n 次の多項式であり、係数を全て調べる事は多項式時間では実行できない。そこで替わりに次の合同式を考える。

$$(X+a)^n \equiv X^n+a \pmod{X^r-1,n} \quad \cdots (※※)$$

このようにすれば、r を小さく取ることで (※※) は多項式時間で検証することができる。X^r-1 で割ったために (※※) を成り立たせる合成数 n が存在するが、今度は複数の a について検証することで n が合成数である可能性を一掃できる。

以上が AKS 法の概略である。次節では具体的にアルゴリズムを紹介し、適当な大きさの自然数 r と適当な個数の a について (※※) の合同式を調べることで正しく素数判定が行われることを確かめる。

3 アルゴリズムとその正当性

以下にアルゴリズムを示す。

入力：自然数 $n(>1)$
Step.1 $n=a^b \quad (a,b\in \mathbf{N}, a,b>1)$ ならば n は合成数。
Step.2 $o_r(n)>4(\log n)^2$ なる最小の r を見つける。
(ただし、$o_r(n):=(\mathbf{Z}_r)^*$ における n の位数)
Step.3 $^{\exists}a\le r \quad s.t. \quad 1<(a,n)<n$ ならば n は合成数。
Step.4 $n\le r$ ならば n は素数。
Step.5 $^{\forall}a\in\{1,2,\cdots,\lfloor 2\sqrt{\varphi(r)}\log n\rfloor\}$ について
$$(X+a)^n \equiv X^n+a \pmod{X^r-1,n}$$
が成り立つならば n は素数。それ以外ならば n は合成数。

まず、このアルゴリズムが多項式時間で実行できることを見る。Step.1 は Bernstein[2] の結果により問題なく処理される。Step.3 以降は r の大きさに依存しており、結局 Step.2 において適当な大きさの r が見つかることだけを示せばよい。

Lemma 3.1
$o_r(n)>4(\log n)^2$ を満たす $r\le\lceil 16(\log n)^5\rceil$ が存在する。

proof.
m 以下の全ての自然数の最小公倍数を $LCM(m)$ で表す。$m\ge 7$ のとき、$LCM(m)\ge$

2^m となる ([3])。もし $^\forall r \leq \lceil 16(\log n)^5 \rceil$ に対して $o_r(n) \leq 4(\log n)^2$ であるとすると、$r|(n^{o_r(n)}-1)$ より

$$LCM(\lceil 16(\log n)^5 \rceil) \leq \prod_{i=1}^{\lfloor 4(\log n)^2 \rfloor} (n^i - 1) < \prod_{i=1}^{\lfloor 4(\log n)^2 \rfloor} n^{4(\log n)^2} \leq n^{16(\log n)^4} \leq 2^{\lceil 16(\log n)^5 \rceil}$$

これは $LCM(\lceil 16(\log n)^5 \rceil) \geq 2^{\lceil 16(\log n)^5 \rceil}$ に矛盾するので、$o_r(n) > 4(\log n)^2$ を満たす $r \leq \lceil 16(\log n)^5 \rceil$ が存在する。■

次に、素数判定が正しく行われることを見る。

Prop 3.2
合成数 n に対して $^\forall a \in \{1, 2, \cdots, l\}$ $(l := \lfloor 2\sqrt{\varphi(r)} \log n \rfloor)$ が (※※) を満たすなら、n は素数の冪である。

Prop3.2 が証明されれば、Step.1 と合わせて素数判定が正しく行われることが分かる。以下では、n は合成数であるとし、$^\forall a \in \{1, 2, \cdots, l\}$ $(l := \lfloor 2\sqrt{\varphi(r)} \log n \rfloor)$ が (※※) を満たすものとする。p を n の素因子、$h(X)$ を $\frac{X^r-1}{X-1}$ の $\mathbf{F}_p$ 上の既約因子とする。

$\mathcal{G} :=$「$\mathbf{F}_p[X]/(h(X))$ 上、$(X+1), \cdots, (X+l)$ が生成する乗法群
(ただし、$(X+1), \cdots, (X+l)$ の中に $h(X)$ と一致するものがあれば除いておく)」
の位数を調べることで、Prop3.2 が成り立つことが示される。

Lemma 3.3
$I = \{n^i p^j | i, j \in \mathbf{Z}_{\geq 0}\}$ とする。$^\forall a \in \{1, 2, \cdots, l\}$ と $^\forall m \in I$ について、

$$(X+a)^m \equiv X^m + a \pmod{X^r - 1, p}$$

が成り立つ。

proof.
まず、

$$\begin{aligned} (X+a)^n &\equiv X^n + a \pmod{X^r - 1, p} \\ (X+a)^p &\equiv X^p + a \pmod{X^r - 1, p} \end{aligned}$$

が成り立つ。
次に、m', m'' が
$\begin{cases} (X+a)^{m'} \equiv X^{m'} + a \pmod{X^r - 1, p} \\ (X+a)^{m''} \equiv X^{m''} + a \pmod{X^r - 1, p} \end{cases}$
を満たすとすると、
仮定より

$$(X+a)^{m'm''} \equiv (X^{m'} + a)^{m''} \pmod{X^r - 1, p}$$

が成り立つ。また、

$$\begin{aligned} (X^{m'} + a)^{m''} &\equiv X^{m'm''} + a \pmod{X^{m'r} - 1, p} \\ \Rightarrow (X^{m'} + a)^{m''} &\equiv X^{m'm''} + a \pmod{X^r - 1, p} \end{aligned}$$

となる。よって、

$$(X+a)^{m'm''} \equiv X^{m'm''} + a \pmod{X^r - 1, p}$$

となる。以上より、

$$^{\forall}m \in I \text{について} (X+a)^m \equiv X^m + a \pmod{X^r - 1, p}$$

が成り立つ。■

Lemma3.3 より、任意の $f(X) \in \{\prod_{a=1}^{l}(X+a)^{e_a} | e_a \in \mathbf{Z}_{\geq 0}\}$ と $m \in I$ に対して

$$(f(x))^m \equiv f(x^m) \pmod{X^r - 1, p}$$

となることが分かる。以下 $f(X)$ はこの形の多項式とする。
$G := \{n^i p^j \bmod r | i, j \in \mathbf{Z}_{\geq 0}\}$, $t := |G|$ とする。

Lemma 3.4
$|\mathcal{G}| \geq \binom{t+l-2}{t-1}$ である。

proof.
$f(X) \neq g(X) \in \mathbf{Z}[X]$ を $\prod_{a=1}^{l}(X+a)^{e_a}$ の形の $(t-1)$ 次以下の多項式とする。もし $\mathcal{G}$ において $f(X) = g(X)$ となるとすると、

$$\begin{aligned} (f(X))^m &= (g(X))^m \quad (m \in I) \\ \Rightarrow f(X^m) &= g(X^m) \end{aligned}$$

$f(Y) - g(Y) \in (\mathbf{F}_p[X]/(h(X)))[Y]$ を考えると、$^{\forall}m \in G$ について X^m は $f(Y) - g(Y) = 0$ の根であるから、$\deg(f(Y) - g(Y)) \geq |G| = t$ となるはずである。ところが、仮定より $\deg(f(Y) - g(Y)) < t$ である。従って、$\mathcal{G}$ において $f(X) \neq g(X)$ となることが分かる。
$\prod_{a=1}^{l}(X+a)^{e_a}$ の形の $(t-1)$ 次以下の多項式は ${}_lH_{t-1}$ 個存在するので、

$$|\mathcal{G}| \geq {}_lH_{t-1} = \binom{t+l-2}{t-1}$$

となる。■

Lemma 3.5
n が p の冪でないならば、$|\mathcal{G}| < \frac{n^{2\sqrt{t}}}{2}$ である。

proof.
$\hat{I} := \{n^i p^j | i, j \in \{0, 1, \cdots, \lfloor\sqrt{t}\rfloor\}\}$ とする。n が p の冪でないので、$|\hat{I}| = (\lfloor\sqrt{t}\rfloor + 1)^2 > t = |G|$ である。よって、$m_1 \equiv m_2 \pmod{r}$ となる $m_1, m_2 \in \hat{I}$ が存在する。このような m_1, m_2 について $(f(X))^{m_1} \equiv f(X^{m_1}) \equiv f(X^{m_2}) \equiv (f(X))^{m_2} \pmod{X^r - 1, p}$ となるので、$\mathbf{F}_p[X]/(h(X))$ において $f(X^{m_1}) = f(X^{m_2})$ である。

$Y^{m_1} - Y^{m_2} \in (\mathbf{F}_p[X]/(h(X)))[Y]$ を考えると、$\mathcal{G}$ の元はすべて $Y^{m_1} - Y^{m_2} = 0$ の根であるので、

$$\deg(Y^{m_1} - Y^{m_2}) \geq |\mathcal{G}|$$

となる。一方、

$$\deg(Y^{m_1} - Y^{m_2}) \leq (np)^{\lfloor\sqrt{t}\rfloor} < \frac{n^{2\sqrt{t}}}{2}$$

であるから、$|\mathcal{G}| < \frac{n^{2\sqrt{t}}}{2}$ が示された。■

最後に、$\binom{t+l-2}{t-1} > \frac{n^{2\sqrt{t}}}{2}$ を示せば、n が p の冪であることが分かる。

Lemma 3.6
$\binom{t+l-2}{t-1} > \frac{n^{2\sqrt{t}}}{2}$ である。

proof.
$t = |G| > o_r(n) = 4(\log n)^2$ より、$t > \lfloor 2\sqrt{t}\log n\rfloor$。
また、$l = \lfloor 2\sqrt{\varphi(r)}\log n\rfloor \geq \lfloor 2\sqrt{t}\log n\rfloor$。
このことから、

$$\begin{aligned}\binom{t+l-2}{t-1} &\geq \binom{2\lfloor 2\sqrt{t}\log n\rfloor - 1}{\lfloor 2\sqrt{t}\log n\rfloor} \\ &\geq 2^{\lfloor 2\sqrt{t}\log n\rfloor} \\ &\geq \frac{n^{2\sqrt{t}}}{2}\end{aligned}$$

となる。■

これでProp3.2が正しいことが証明された。

参考文献

[1] M. Agrawal, N. Kayal, N. Saxena, "Primes is in P. Revised paper version", http://www.cse.iitk.ac.in/news/primality.html

[2] D. J. Bernstein, "Detecting perfect powers in essentially linear time", *Mathematics of Computation 67, 1253-1283,* http://cr.yp.to/lineartime.html#powers

[3] M. Nair, "On Chebyshev-type inequalities for primes", *American Journal of Mathematics 89, 126-129.*